亚冬会赛事信息系统遭到境外网络攻击

哈尔滨公安通缉3名美国特工

今年哈尔滨亚冬会前后，赛事信息系统遭到来自境外网络攻击270167次。

哈尔滨公安局组织国家计算机病毒应急处理中心和360等境内网络安全机构技术专家，迅速开展网络攻击溯源调查。追查到美国国家安全局（NSA）的3名特工凯瑟琳·威尔逊（Katheryn A. Wilson）、罗伯特·思内尔（Robert J. Snelling）、斯蒂芬·约翰逊（Stephen W. Johnson）和两所美国高校，参与实施了此次网络攻击。

4月15日，哈尔滨公安局发布公开悬赏，通缉3名美国国家安全局特工。

视觉中国供图

冰雪盛会背后的“网络暗战”

2月3日，是哈尔滨第九届亚冬会首个比赛日。当天男子冰球组比赛正酣，针对赛事系统的网络攻击也在悄然增加。

国家计算机病毒应急处理中心高级工程师杜振华此前提到，针对赛事信息系统的网络攻击主要来源于美国，数量超过17万次，占比超过60%。他介绍，从以往的网络攻击案例中获悉，美国的情报机构频繁地使用荷兰或者其他欧洲国家的网络主机作为跳板对目标实施攻击，所以看到的是来自荷兰的攻击数量比较多，但是背后的实际攻击源可能也是来自美国。

调查也发现，此次美国国家安全局特定入侵行动办公室为了掩护其攻击来源和保护网络武器安全，依托所属多家掩护机构购买了一批不同国家的IP地址，并匿名租用了一大批位于欧洲、亚洲等国家和地区的网络服务器。

攻击行为主要集中在亚冬会注册系统、抵离管理系统、竞赛报名系统等重要信息系统。这些系统关系到赛事的重要信息发布、人员和物资的调配、赛事的组织管理，同时也保存有大量赛事相关人员身份敏感信息。

另外，美国国家安全局还掌握着大量不为人知的0Day漏洞。通过这些漏洞可以攻击操作系统后植入特定木马，进行潜伏预埋，类似“定时炸弹”，随时可以通过发送加密字节数据进行唤醒。

边亮是360高级威胁研究院副院长，他带领团队100多名成员参与此次溯源调查。

团队发现，此次针对亚冬会的网络攻击，出现了AI化趋势，这是此前并未出现过的攻击方式。在传统攻击方式中，攻击前的侦察阶段靠人工筛选目标、侦察目标情况、分析行为偏好，然后开展攻击，整个过程时间成本非常高。

此次技术团队对攻击代码研判后发现，在漏洞探寻、流量监测等方面，部分代码明显由AI书写，在攻击过程中自动、快速编写动态代码实施攻击。

这意味着攻击者利用AI，可复制出大量数字黑客，在多个目标点进行漏洞探寻、自动设计作战方案和生成攻击工具，实施无差别攻击。更令人担心的是，数字黑客反应速度远超人类，对国家安全防护防御体系构成巨大挑战。

看不见的攻防和博弈

在这场隔着屏幕的较量中，发现黑客的踪迹、捕捉其行踪、定位并最终确定其身份，像是一场高科技版的“猫鼠游戏”。

在边亮看来，较量的起点常常可能只是一次流量异常——例如，某台电脑在深夜频繁向外发送大量数据，或者试图连接陌生服务器。这些异常流量就像网络世界中的“脚印”，虽然细微，但对于经验丰富的网络安全专家来说，却是重要的线索。

网络攻击的蛛丝马迹常常隐藏在海量的数据日志中。发现异常是第一步，接下来要溯源它的路径，找到它最初出发的地方。通过仔细检查每一个数据包的来源、去向和内容，试图拼凑出攻击者的行动轨迹。

大数据对比分析也至关重要。通过将捕捉到的信息，与多年沉淀下来的数据库中已知的黑客行为模式进行比对，技术专家们分析“这种攻击手法是不是某个黑客组织的典型风格？这个IP地址之前有没有被报告过？”可以大致判断出攻击者的身份，甚至可能找到其真实身份。

“抓住对方的失误”往往是找到攻击者的关键。边亮介绍，黑客在实施攻击时会使用一些特定的工具、组件或者协议规范，这就像他们的“指纹”，可以通过技术手段被识别出来。在开发攻击工具时，常会赋予其独特名字或代号，就像名片，或者是使用的跳板偶尔失灵，这些信息可能在攻击中泄露，进而成为暴露身份的线索。

在长期的攻防战中，网络安全专家们也总结出了一些作息规律——大部分实施网络攻击的人往往不会在周末、圣诞节等西方国家的节假日活动。这似乎代表着对方的攻击是某种职务行为。

最终，经过持续的攻坚溯源，成功锁定了参与网络攻击亚冬会的美国国家安全局3名特工。据了解，实施此次网络攻击行动的组织是美国国家安全局信息情报部（代号S）数据侦察局（代号S3）下属特定入侵行动办公室（Office of Tailored Access Operation，简称“TAO”，代号S32）。技术团队同时发现，具有美国国家安全局背景的美国加利福尼亚大学、弗吉尼亚理工大学也参与了本次网络攻击。

关键基础设施单位亟须提高自身防御能力

据哈尔滨公安局消息，美国国家安全局主要围绕特定应用系统、特定关键信息基础设施、特定要害部门开展网络渗透攻击，涵盖数百类已知和未知攻击手法，攻击方式超前，包括未知漏洞盲打、文件读取漏洞、短时高频定向检测攻击、备份文件及敏感文件及路径探测攻击、密码穷举攻击等，攻击目标、攻击意图明显。

技术团队还发现，美国国家安全局向我国多个基于Windows操作系统的特定设备发送未知加密字节，疑为唤醒、激活Windows操作系统提前预留的特定后门。

360集团创始人、董事长周鸿祎表示，早在2022年，360就发现了NSA和CIA对我国包括西北工业大学、武汉市地震监测中心等发起的网络攻击，并成功溯源、上报有关部门。截至目前，360已经帮助国家发现56个境外国家级APT（高级持续性威胁）组织。

据了解，APT通常是由国家级或准国家级的黑客组织发起，往往针对我国政府、行业龙头企业、大学、医疗机构、科研单位等进行网络攻击，其目标是获取高价值信息或破坏关键基础设施，具有复杂且隐蔽、攻击工具武器化等特点。而360之所以能够成功溯源，得益于近20年来积累的全世界最大规模安全大数据，建立了全面的攻击样本和行为知识库，以及攻击手法的关联基因库。

周鸿祎认为，随着大模型的发展，美国情报机构的大规模网络攻击行动已进入AI时代，无论是自动化漏洞挖掘还是智能恶意代码生成，尤其是大模型的发展不仅大幅度提升了网络攻击效率，更突破了传统攻击手段的时空限制，把网络战推向了更加智能化、自动化的阶段。

而当前国际形势复杂动荡，伴随着大国博弈的加剧，网络空间的军事化进程也明显加快。网络战被越来越多的国家或力量当作攻击他国的“利器”，网络空间的安全威胁更具杀伤性和破坏力。

在国家级黑客组织的威胁下，广大关键基础设施单位亟须提高自身防御能力。

中方将继续采取必要措施保护自身网络安全

中国外交部发言人林剑15日表示，中方将继续采取一切必要措施保护自身的网络安全。

当日例行记者会上，有记者问：今天哈尔滨市公安局发布通告，悬赏通缉参与在第九届亚冬会期间对赛事信息系统和黑龙江省关键信息基础设施开展网络攻击的美国国家安全局有关人员。中方对此有何评论？

林剑表示，中方注意到有关报道。此前，中方已经多次阐述立场。在第九届亚冬会期间，美国政府针对赛事信息系统和黑龙江省内关键信息基础设施开展网络攻击，对中国关键信息基础设施、国防、金融、社会、生产以及公民个人信息安全造成严重危害，性质十分恶劣。中方谴责美国政府的上述恶意网络行为。

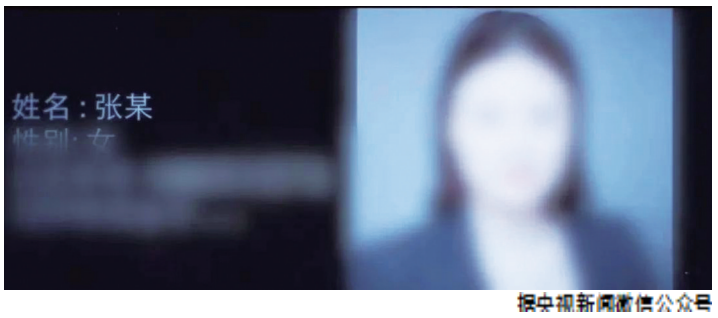
林剑说，中方敦促美方在网络安全问题上采取负责任的态度，停止对中方实施网络攻击，停止对中方无端抹黑和攻击。

综合新华社、新京报

国家部委涉密会议现场

一声“吧嗒”，她的间谍身份曝光

4月15日，国家安全部披露重磅案例，某国家部委工作人员张某，多次潜入涉密会议室安放录音设备。当录音笔意外坠落，警觉的参会人员及时报告了情况，阻止了她疯狂窃密……



报央视新闻微信公众号

某部委工作人员隐匿身份，主动投敌疯狂窃密

某重点单位的一次涉密会议上，突然“吧嗒”一声，一支正在工作的录音笔掉落在座椅下方，从痕迹看，这支录音笔被用强力胶布粘在座椅下，因多次使用黏性减弱而掉落。

参会人员高度警觉，立刻向单位领导报告。单位认为此事非同小可，于是向国家安全机关报告了相关情况。

经查，该单位工作人员张某有重大嫌疑。国家安全机关同时发现，张某和另一个已经在侦的案件嫌疑人具有极高的关联度。原来，早在一个多月前，国家安全机关就发现有人主动与某境外间谍情报机关联系，想提供涉密文件。

国家安全机关就此立即深入调查，并案开展工作，依法对张某实施突击审查，随着案情的逐渐清晰，令人震惊的是，该人与张某是同一个人。

张某，女，出生于一个知识分子家庭，大学毕业后，先后就职于知名高校、市直单位，直至国家部委。

从高中起，张某就开始偷偷浏览一些境外网站，主动寻找和接触反动思想，自甘沉沦。走上涉密岗位后，张某不但丝毫没有收敛，反而还因个人矛盾，将窃取和出卖国家秘密作为报复同事、单位乃至国家和社会的手段。

她通过技术手段隐匿身份，主动向境外间谍情报机关发送投靠邮件，在对方指挥下，疯狂出卖我重要领域国家秘密。

多次潜入内部会议室放录音笔，携带海量文件叛逃前被抓获

张某利用单位管理漏洞，长期从单位办公系统违规下载文件，还擅自携带手机进入涉密场所拍摄涉密文件，趁办公室无人之机，窃取拷贝同事计算机内的电子文件，并多次潜入内部会议室安放录音笔，对会议内容进行秘密录音。

至案发时，张某累计窃取的内部文件资料已近30万份。

窃密录音笔被发现后，张某迅速办理了出境证件，随时准备携带窃取的海量内部文件叛逃。在张某所在单位配合下，国家安全机关及时对其实施控制，防止危害进一步扩大，等待张某的是法律的严惩。

张某重大间谍案的发生，暴露出其所在单位作为国家重要领域要害部门，防谍保密主体责任不落实，制度执行不严，在干部教育、管理、监督等方面存在严重问题漏洞。

纪检检查部门启动倒查问责，对案件直接涉及的12名失职失责领导干部和责任人员分别给予党纪政务处分。 综合央视、国家安全部网站